IN THE CLAIMS:

Please AMEND claims 1-35; and

Please ADD claim 36, as shown below.

1. (Currently Amended) A method ~~for providing secure access to a packet data network, said method~~ comprising:

receiving a message from a terminal device connected to ~~said~~ a packet data network;

deriving a first source information from said message;

deriving a second source information;

comparing said first source information and second source information; ~~and~~

initiating a protection processing based on a result of said comparing; and

providing secure access to said packet data network based on said protection processing.

2. (Currently Amended) A method ~~for providing secure access to a packet data network, said method~~ comprising:

receiving a message from a terminal device connected to ~~said~~ a packet data network;

deriving a first source information from said message;

deriving a second source information;

comparing said first source information and second source information; ~~and~~

initiating a protection processing based on a result of said comparing; and

providing secure access to said packet data network based on said protection processing.

3. (Currently Amended) ~~A~~ The method according to claim 1, wherein said second source information is a source address information derived from a packet data unit configured to convey said message, or from a security association set up between said terminal device and said packet data network.

4. (Currently Amended) ~~A~~ The method according to claim 1, wherein said protection processing comprises a processing for dropping said message if the result of said comparing is that said first source information and said second source information do not indicate the same location.

5. (Currently Amended) ~~A~~ The method according to claim 1, wherein said protection processing comprises a processing for dropping said message if said comparing leads to the result that said first source information and said second source information do not match.

6. (Currently Amended) ~~A~~ The method according to claim 1, wherein said first source information is an internet protocol address.

7. (Currently Amended) ~~A~~ The method according to claim 6, wherein said message is a session initiation protocol message.

8. (Currently Amended) ~~A~~ The method according to claim 1, wherein said second source information is at least a part of an internet protocol source address of an internet protocol datagram.

9. (Currently Amended) ~~A~~ The method according to claim 1, wherein said second source information is at least a part of an internet protocol source address of an internet protocol datagram.

10. (Currently Amended) ~~A~~ The method according to claim 3, wherein said second source information is an internet protocol address bound to an integrity key of said security association.

11. (Currently Amended) ~~A~~ The method according to claim 10, wherein said internet protocol address is stored in a database of a proxy server configured to route said message to said packet data network.

12. (Currently Amended) ~~A~~ The method according to claim 10, wherein said message is conveyed using a session initiation protocol level protection function.

13. (Currently Amended) A network element ~~for providing secure access to a packet data network~~, ~~said network element~~ comprising:

a receiving ~~means for~~unit configured to ~~receiving~~ receive a message from a terminal device connected to said network element;

a deriving ~~means for~~unit configured to ~~deriving~~ derive a first source information from said message, and for deriving a second source information;

a comparing ~~means for~~unit configured to ~~comparing~~ compare said first source information and second source information; and

a protecting ~~means for~~unit configured to ~~initiating~~ initiate a protection processing based on a comparing result of said comparing unit ~~means~~and to provide secure access to a packet data network based on said protection processing.

14. (Currently Amended) ~~A~~ The network element according to claim 13, wherein said deriving ~~means~~ unit is configured to derive said second source information from a packet data unit configured to derive said message or from a security association set up between said terminal device and said network element.

15. (Currently Amended) ~~A~~ The network element according to claim 13, wherein said deriving ~~means~~ unit is configured to derive said first source information from a header portion of said message.

16. (Currently Amended) ~~A~~ The network element according to ~~any one of claims 13~~ claim 13, wherein said protecting ~~means~~ unit is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate a same location.

17. (Currently Amended) ~~A~~ The network element according to ~~any one of claims 13~~ claim 13, wherein said protecting ~~means~~ unit is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.

18. (Currently Amended) ~~A~~ The network element according to ~~any one of claims 13~~ claim 13, wherein said deriving ~~means~~ unit is configured to read said second source information from a database provided at said network element.

19. (Currently Amended) ~~A~~ The network element according to ~~any one of claims 13~~ claim 13, wherein said deriving ~~means~~ unit is configured to derive said second source information by extracting an internet protocol source address from an internet protocol datagram.

20. (Currently Amended) ~~A~~ The network element according to claim 13, wherein said network element is a proxy server.

21. (Currently Amended) ~~A~~ The network element according to claim 20, wherein said proxy server is a proxy call state control function of an internet protocol mobility subsystem.

22. (Currently Amended) ~~A~~ The method according to claim 2, wherein said second source information is a source address information derived from a packet data unit configured to convey said message, or from a security association set up between said terminal device and said packet data network.

23. (Currently Amended) ~~A~~ The method according to claim 2, wherein said protection processing comprises a processing for dropping said message if the result of said comparing is that said first source information and said second source information do not indicate the same location.

24. (Currently Amended) ~~A~~ The method according to claim 23, wherein said protection processing comprises a processing for dropping said message if the result of said comparing is that said first source information and said second source information do not match.

25. (Currently Amended) ~~A~~ The method according to claim 2, wherein said first source information is an internet protocol address.

26. (Currently Amended) ~~A~~ The method according to claim 2, wherein said message is a session initiation protocol message.

27. (Currently Amended) ~~A~~ The method according to claim 2, wherein said second source information is at least a part of an internet protocol source address of an internet protocol datagram.

28. (Currently Amended) ~~A~~ The method according to claim 2, wherein said message is conveyed using a session initiation protocol-level protection function.

29. (Currently Amended) ~~A~~ The network element according to claim 14, wherein said deriving ~~means~~ unit is configured to derive said first source information from a header portion of said message.

30. (Currently Amended) ~~A~~ The network element according to claim 14, wherein said protecting ~~means~~ unit is configured to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate the same location.

31. (Currently Amended) ~~A~~ The network element according to claim 14, wherein said protecting ~~means~~ unit is configured to initiate a processing for dropping said message if

said comparing result indicates that said first source information and said second source information do not match.

32. (Currently Amended) ~~A~~ The network element according to claim 14, wherein said deriving ~~means~~ unit is configured to read said second source information from a database provided at said network element.

33. (Currently Amended) ~~A~~ The network element according to claim 14, wherein said deriving ~~means~~ unit is configured to derive said second source information by extracting an internet protocol source address from an internet protocol datagram.

34. (Currently Amended) ~~A~~ The network element according to claim 14, wherein said network element is a proxy server.

35. (Currently Amended) ~~A~~ The network element according to claim 34, wherein said proxy server is a proxy call state control function of an internet protocol mobility subsystem.

36. (New) A network element, comprising:

receiving means for receiving a message from a terminal device connected to said network element;

deriving means for deriving a first source information from said message, and for deriving a second source information;

comparing means for comparing said first source information and second source information; and

protecting means for initiating a protection processing based on a comparing result of said comparing means and for providing secure access to a packet data network based on said protection processing.